Research Paper | Education | E-ISSN No : 2454-9916 | Volume : 10 | Issue : 3 | March 2024

NETWORK TRAFFIC BASED RANSOMWARE DETECTION

Sivaguru R.[1], Srinath R.[2], Sathiya Rubha M.[3], Yasmin Banu R.[4], Sathish Kumar K.[5]

[1] Assistant Professor, Department of Computer Science and Engineering, Knowledge Institute of Technology, Salem, Tamilnadu
[2, 3, 4, 5] UG Student, Department of Computer Science and Engineering, Knowledge Institute of Technology, Salem, Tamilnadu

ABSTRACT

Introduces a novel framework designed to bolster cybersecurity defenses against ransomware attacks. This system integrates an advanced Intrusion Detection and Prevention System (IDPS) with cutting-edge machine learning algorithms to efficiently identify and neutralize ransomware threats in real-time. By analyzing network traffic and system behavior, the IPS identifies patterns and anomalies that signify a potential ransomware attack, leveraging a comprehensive database of known ransomware signatures and behavior profiles. Upon detecting a threat, the system not only alerts the network administrators but also takes preemptive actions to isolate the attack, preventing the ransomware from spreading and encrypting files. This proactive approach significantly reduces the risk of data loss and operational downtime, enhancing the overall security posture of organizations. The deployment of this IDPS represents a crucial advancement in the fight against ransomware, offering a dynamic and adaptive solution to a rapidly evolving cyber threat landscape.

KEYWORDS: Ransomware Detection, Cybersecurity, Wireshark, Tshark, Intrusion Prevention System

1. INTRODUCTION

Ransomware has emerged as one of the most pernicious and prevalent cyber threats facing individuals, businesses, and governments worldwide. With its ability to encrypt critical data and demand ransom payments for decryption keys, ransomware poses significant risks to data integrity, operational continuity, and financial stability.Detecting ransomware poses formidable challenges for cybersecurity practitioners due to its stealthy nature and constantly evolving tactics. Traditional signature-based antivirus solutions are often ineffective against polymorphic ransomware variants that mutate to evade detection. Moreover, ransomware operators employ encryption techniques and obfuscation methods to conceal their malicious activities, rendering anomaly-based detection approaches less reliable. Furthermore, the increasing prevalence of fileless ransomware, which operates solely in memory without leaving traces on disk, complicates detection efforts further. Intrusion Detection and Prevention Systems (IDPS) have emerged as critical components of modern cybersecurity architectures, providing real-time monitoring, analysis, and response capabilities to detect and mitigate cyber threats. By analyzing network traffic and system logs, IDPS can identify suspicious patterns, anomalies, and indicators of compromise associated with ransomware activity. Additionally, IDPS solutions can leverage threat intelligence feeds and machine learning algorithms to enhance detection accuracy and adaptability, enabling proactive defense against emerging ransomware threats. ransomware represents a pervasive and evolving cybersecurity challenge, necessitating proactive detection and mitigation strategies. By leveraging Intrusion Detection and Prevention Systems (IDPS), organizations can enhance their resilience against ransomware attacks, safeguarding critical assets and preserving operational continuity.

2. MALWARE

Defining Malware

Malware, short for malicious software, encompasses a broad range of software programs designed to harm, exploit, or otherwise perform unauthorized actions on a computer system or network. It is the collective term for viruses, worms, trojans, ransomware, spyware, adware, and many other types of harmful code. Malware authors craft these programs for various malicious purposes, including stealing sensitive data, damaging system resources, conducting espionage activities, displaying unwanted advertisements, or hijacking core computing functions for nefarious ends. Malware can infiltrate systems through numerous vectors. Common methods include phishing emails, malicious attachments or links, compromised websites, software vulnerabilities, and through other software installations. Once inside a system, malware can execute a variety of destructive actions: it can encrypt files to demand ransom (ransomware), log keystrokes to capture passwords (keyloggers), create backdoors for future access, or even utilize system resources for cryptocurrency mining. The sophistication of malware has evolved dramatically, leveraging advanced techniques to evade detection by security software, exploit zero-day vulnerabilities, and masquerade as legitimate software. The arms race between cybersecurity professionals and malware authors is ongoing, with each new defense met by innovative methods to circumvent it. Consequently, protecting against malware requires a combination of up-to-date security software, regular system patches, user education, and adherence to best cybersecurity practices.

3. RANSOMWARE

What is Ransomware?

Ransomware is a type of malware that encrypts a victim's

data, making it inaccessible, and then demands a ransom from the victim to restore access. The ransom is typically paid in cryptocurrency, making it difficult for law enforcement to trace and apprehend the attackers. Ransomware attacks have become increasingly sophisticated, with attackers employing various methods to infect systems, including phishing emails, exploiting software vulnerabilities, and using malicious apps or drive-by downloads.

There are two main types of Ransomwares:

Encrypting ransomware: This type encrypts the victim's data, making it inaccessible until the ransom is paid. The attacker then demands a ransom in exchange for the decryption key.

Non-encrypting ransomware: Also known as screen-locking ransomware, this type locks the victim's entire device, usually by blocking access to the operating system, and demands a ransom to unlock it.

Ransomware attacks can also take on more sinister forms, such as:

Leak ware/Doxware: This type of ransomware steals sensitive data and threatens to publish it online if the ransom is not paid.

Mobile ransomware: Affects mobile devices, often delivered via malicious apps or drive-by downloads. It is typically non-encrypting due to the prevalence of automated cloud data backups on mobile devices.

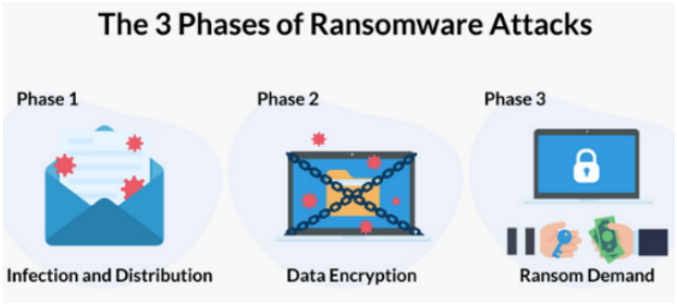
Wipers/destructive ransomware: Threatens to destroy data if the ransom isn't paid, with some variants even destroying data even if the ransom is paid.

Scareware: Tries to scare users into paying a ransom by posing as a law enforcement agency or spoofing a legitimate virus infection alert.

Ransomware attacks have evolved significantly over the years, with attackers employing more sophisticated techniques to gain access and encrypt data. The emergence of cryptocurrency has made ransomware attacks more appealing to attackers, as it simplifies the ransom payment process.

How Ransomware Attack Works

After a device is exposed to the malicious code, the ransomware attack proceeds as follows. Ransomware can remain dormant on a device until the device is at its most vulnerable, and only then execute an attack.It can take as little as three days for ransomware to infiltrate and infect systems. This ransomware playbook flowchart outlines the different stages of an attack, so you know where to improve defenses and implement strong controls and policies.



Phase 1: Infection and Distribution

The first phase of a ransomware attack starts with accessing an organization's network. This may be done in several ways, with phishing emails being the primary method. In this case, cybercriminals send malicious emails with links or attachments that, once accessed, download and execute the malware on the victims' terminals. It only takes a negligent click to turn the tentative into a costly breach.Another way to spread infection into the enterprise's systems, especially in today's work-from-home landscape, is by taking advantage of the Remote Desktop Protocol. To do so, it is enough for attackers to either steal or guess a target's login credentials. This is especially easy if potential victims reuse their passwords for multiple accounts or use one of the weak ones that attackers.

Once cybercriminals identify the correct ID/password combination, they can gain remote access to the user's computer, enabling them to download and execute the malware on the terminal and distribute it across the organization.Other attempts may include exploiting certain software vulnerabilities. A well-known example here is how the WannaCry ransomware used the Eternal blue exploit, a software vulnerability in Microsoft's Windows operating systems (OS) . The exploit enabled the bad actors to execute arbitrary code and take over a system through specially crafted packages.

Phase 2: Data Encryption

Once bad actors have gained access to the network, it is time to start the second phase, data encryption. This means that malware encrypts accessible files with a key known solely by the attacker. The encrypted ones replace the old, original files and, in some cases, backups and shadow copies are deleted. Using this approach, cybercriminals ensure that recovering data is even more complicated for organizations.Ransomware scans and map's locations for targeted file types, including locally stored files, and mapped and unmapped network-accessible systems. Some ransomware attacks also delete or encrypt any backup files and folders. It Doesn't allow you to access the System or Computer by the user

Phase 3: Ransom Demand

After cybercriminals have encrypted the files, it is time for them to make their demand. This may happen in different ways, depending on the bad actor's approach. One of the most common methods is changing a computer's background to a ransom note which offers to provide the victim the key to access their files in exchange for cryptocurrency. Another option would be to add text files to the encrypted directories so that, when users open them, they receive the ransom message.

If the organization pays the ransom, the cybercriminal may provide a copy of the encryption key or of the private key that protects the symmetric encryption key, as well as the decryptor program that victims may use to restore access to the original files and the system. All that needs to be done, at this point, is to enter the information into the program.Although these 3 phases can be found in all ransomware attempts, there are types of attacks that might be different or include additional measures. One relevant example is Maze, the ransomware that uses file scanning, registry information, and data theft before data encryption.

Why Ransomware is on Rise

To carry out a successful attack, the cybercriminals must deliver some kind of malware that encrypts computers, files, and even entire networks. Once the data has been encrypted, a key is needed to unlock the files. The attackers can then contact the business saying that they will only decrypt the files for a payment, most often in cryptocurrency.In 2021, several factors led to an unprecedented growth in these cyberattacks. Emails and fake websites were the primary delivery tools, and concern about the COVID-19 Pandemic provided a convenient topic for clickbait. People were searching for details on the subject and were less careful about clicking on an attachment or embedded link. Once an unsuspecting employee clicked on a corrupt link or attachment, the device or system had already been infected.In addition, the growth of cryptocurrencies provided an easier means to carry out anonymous ransom transactions. More people were familiar with the technology, so demanding a Bitcoin transaction was not unreasonable. Some criminal groups even provided step-by-step instructions for conducting a cryptocurrency payment.Encrypting and ransoming data used to require people with high-level technical skills. But some of these cybercriminals have discovered that it is actually easier and more profitable to hire out their abilities (a Ransomware-as-a-Service model) than carry out individual attacks. Ransomware-as-a-Service means that even the most novel hackers can execute highly sophisticated, targeted cyberattacks. Ransomware has become a lucrative business for cybercriminals.

What Happens when Ransomware Attacks to Organization

Ransomware attacks pose a significant threat to organizations, impacting their operations, financial health, and reputation. These cyber-attacks involve the unauthorized access to a system, where attackers encrypt files, rendering them inaccessible to the rightful owner. They then demand a ransom, typically in cryptocurrency, to decrypt the files. The consequences of such attacks are far-reaching and can severely affect businesses of all sizes.

Impact on Operations and Revenue

Ransomware attacks can halt operations, leading to significant productivity loss and revenue decline. Even with functional backups, restoring affected systems can take hours to days, further impacting business continuity.The cost of ransom payments can be substantial, ranging from hundreds of thousands to millions of dollars. Additionally, organizations may incur expenses for remediation, including new hardware, software, and incident response services. The financial strain can lead to layoffs, business closures, and even bankruptcy for small businesses.

Reputation and Brand Damage

A successful ransomware attack can severely damage an organization's reputation. Customers may perceive the attack as an indication of weak security practices, leading to a loss of trust and potential business. This can result in a loss of customers and a decrease in market value.Studies have shown that 53% of organizations reported brand and reputation damage as a result of a ransomware attack. This can lead to a loss of competitive advantage and increased legal and compliance exposure.

Legal and Compliance Implications

Ransomware attacks can lead to the loss of sensitive customer data, including Personally Identifiable Information (PII) and trade secrets. This can result in legal action, fines, and penalties under data protection regulations.The financial impact of a ransomware attack can lead to increased insurance premiums, further straining the organization's financial health.

4. THREAT DETECTION

In the ever-evolving battle against ransomware, a layered defence strategy is essential. Network traffic analysis (NTA) and intrusion detection systems (IDS) play complementary roles in this fight, offering a comprehensive approach to ransomware detection.

NTA functions by dissecting network data packets, searching for patterns that deviate from normal behaviour. This includes sudden spikes in file encryption activity, a surge of outbound connections to unknown IP addresses, or specific file access patterns associated with ransomware. NTA can leverage signature-based detection, matching known malicious patterns, or anomaly-based detection, identifying deviations from established baselines. Advanced implementations even utilize machine learning to continuously refine detection accuracy.On the other hand, IDS operates by monitoring network traffic for activities that violate predefined security rules. It can detect and potentially block suspicious behaviours like attempts to exploit vulnerabilities in systems, communication with ransomware command-and-control (C&C) servers, or unauthorized access attempts. The effectiveness of IDS hinges on maintaining up-to-date signatures and rules to stay ahead of evolving threats. The true strength lies in how these two systems work together. NTA provides a broader perspective on network behaviour, potentially identifying early warning signs of a ransomware attack. Meanwhile, IDS focuses on specific malicious activities often associated with ransomware deployment. This synergy offers several advantages: NTA can flag suspicious traffic, prompting IDS to investigate further. If malicious activity is confirmed, IDS can potentially block it, preventing the attack from progressing.This combined approach offers several benefits. Proactive detection can occur before crucial data is encrypted, significantly reducing the impact of the attack. Additionally, both systems provide improved threat visibility across the entire network. Faster response times are also achievable, allowing security teams to swiftly contain

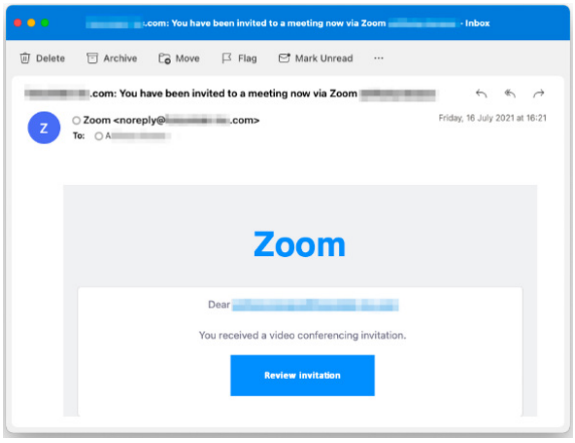
the attack and minimize damage.However, it's important to acknowledge limitations. Configuring and interpreting NTA results requires a certain level of expertise. Similarly, IDS relies on constantly updated signatures, which might not cover zero-day attacks. Both systems can also generate false positives, requiring investigation to avoid unnecessary disruption.To further strengthen defences, consider integrating NTA and IDS with a Security Information and Event Management (SIEM) system. This enables centralized logging and analysis of security events, providing a holistic view of potential threats. Additionally, maintaining up-to-date signatures and rules for both IDS and NTA is crucial. Finally, fostering a culture of cybersecurity awareness among employees plays a vital role. Educating staff on how to identify social engineering tactics used to spread ransomware can significantly reduce the attack surface.By combining network traffic analysis and intrusion detection systems, organizations can significantly bolster their defences against ransomware attacks. This layered approach offers proactive detection, improved threat visibility, and faster response times, ultimately safeguarding valuable data and minimizing business disruptions.

Most Common Attack Vectors of Ransomware

Email Phishing

The most widely used attack vector is email phishing. In this case, attackers use email lists to send malicious links to an organization's employees. This might seem like a significant effort, but it has become quite simple with software automation. The principle behind the strategy is that it only takes one person to click on the link to enable cyber attackers to infiltrate an entire organization.

As phishing has evolved, bad actors have developed several more efficient approaches. One of the most popular is Spear Phishing a version in which cybercriminals use public information about their targets, simulating a relationship between the email sender and the receiver. This is usually done by using information available on social media accounts, like LinkedIn, to create emails that inspire trust, thus increasing the chance of clicking on links or downloading files.These stakeholders are usually less likely to commit negligence, so it is essential to make messages look like they are coming from a trustworthy source.



Top Reasons Why Employees Fall for Spear Phishing

Bad actors don't focus solely on the technical side of attacks but also emotional factors. Since they need to take advantage of people's trust, they use Social Engineering Technique to create emails that make sense from a corporate perspective and have the same tone of voice and format as legitimate messages. They lower victims' skepticism and increase their chances of a successful spear phishing attempt.To add that extra layer of emotion that sparks quick actions, bad actors also use keywords meant to suggest urgency. Terms like "immediate action required," "urgent," and "overdue notice" not only get the receiver's attention but also send a solid call to action, demanding for something to be done. Other emails take advantage of people's vulnerabilities and desires, as they present opportunities that are not real, such as winning a deal, being offered a bonus, or a promotion.To go even further and remove any doubt for potential victims, bad actors put in the extra effort and adopt an organization's communication style, focusing on workflows and processes to which employees are accustomed. Cyber attackers study users' behaviours and correspondence patterns and replicate standard emails that impersonate colleagues, Suppliers or Partners. Another reason why these attempts are particularly successful is because, especially in the corporate environment, employees need to make quick decisions. Opening an email, for example, is often an automatism since users receive tens or even hundreds of messages per day. People check messages, access links, and download attachments while taking phone calls or scheduling meetings. With so much multitasking, it is sometimes just a matter of time before someone makes a mistake.

Remote Desktop Protocol Compromise

By allowing users to interact with their desktops from remote locations, Remote Desktop Protocol (RDP) offers a high level of convenience to employees from different departments. This solution enables them to enjoy working from home while proceeding with their tasks. Moreover, it is also a preferred choice of IT professionals who only need to connect remotely to access someone's computer, troubleshoot problems, install updates, etc.At the same time, this type of solution comes with its share of challenges, as the Remote Desktop Protocol increases an organization's attack surface. RDP is a significantly Important Gateway for Actors. RDP often goes hand in hand with Brute-Force Attacks through which bad actors use trial-and-error to guess login information and access computers. Another tactic that works for unauthorized RDP access is purchasing credentials on the dark web.

Replacing legacy software or updating existing tools is a challenge in most companies because employees are often resistant to change. Many organizations still use unpatched software versions. These environments are excellent for bad actors since unpatched vulnerabilities open the door for attacks without requiring any credentials. Zero Day Vulnerabilities can be exploited by bad actors to launch an attack, before potential victims have the chance to apply security updates to protect against it.

5. PREVENTION METHODS

Regularly update your devices

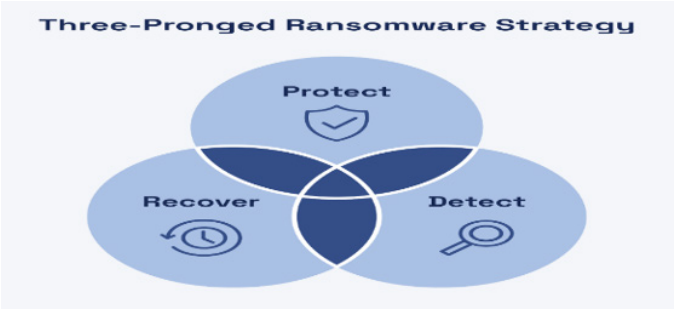
Cybercriminals use known weaknesses to hack your devices. Updates have security upgrades so known weaknesses can't be used to hack you. You should always update your system and applications when prompted. You can also turn on automatic updates on some devices and applications so that updates happen without your input.If you have a server or Network Attached Storage (NAS) device in your network, make sure they are regularly updated too. If you are unsure how to update your NAS refer to the manufacturer's guidance or speak to an IT professional.

Set up and perform regular backups

A backup is a digital copy of your most important information (e.g. photos, customer information or financial records) that is saved to an external storage device or to the cloud.The best recovery method from a ransomware attack is to restore from an unaffected backup. Regularly backup your files to an external storage device or the cloud. Backing up and checking that backups restore your files offers peace of mind.

Implement access controls

Controlling who can access what on your devices will help reduce the risk of ransomware. It will also limit the amount of data that ransomware attacks can encrypt, steal, and delete.To do this, give users access and control only to what they need. This can be done by making sure each person who uses the device has the right type of account.There are two types of accounts you can set up on Microsoft Windows and Apple macOS; a standard account and an administrator account. Everyday users should have a standard account. Only those who need to should have an administrator account. Consider creating a standard account to use as your main account as they are less susceptible to ransomware. It's also important that users don't share their login details for accounts



Email vigilance

Phishing emails, disguised as legitimate messages, are a common way to deliver ransomware. Here's the golden rule: never click on suspicious links or open attachments from unknown senders. Even emails from seemingly familiar contacts can be spoofed, so be wary of anything unexpected or containing urgency. Think before you click – a moment of caution can prevent hours of frustration.

Security software

acts as your digital sentry. Invest in a reliable antivirus and anti-malware solution with good ransomware protection ratings. These tools can detect and block ransomware attempts before they encrypt your data. Consider them your security guard, constantly on patrol to identify and stop intruders.

Network segmentation

Imagine dividing your network into smaller, isolated zones. If one zone gets compromised, the damage is contained, preventing the ransomware from spreading throughout your entire system. Think of it as compartmentalizing your house – a fire in one room doesn't engulf the whole structure.

Limited user privileges

Grant users only the minimum level of access needed to perform their tasks. This principle of "least privilege" reduces the potential impact of a ransomware attack, since a compromised account with limited access can cause less damage. It's like giving house keys only to specific rooms, not the entire building.

Security awareness training

Empower your employees to be your frontline defence Train them on how to identify and avoid phishing attempts, suspicious attachments, and other social engineering tactics used by ransomware attackers. Knowledge is power – equip your team to recognize and respond to potential threats.

Regular security testing

Don't wait for disaster to strike. Schedule regular security assessments to identify vulnerabilities in your systems that attackers might exploit. Think of this as proactively inspecting your house for weak points before a break-in attempt.

By implementing these strategies, you build a formidable defence against ransomware. Remember, prevention is always cheaper and less disruptive than recovery.

6. WHO IS THE TARGET

They Hold Sensitive and Classified Data

State agencies are responsible for massive amounts of data, and much of it is sensitive and vital for national security as well as the security of individual citizens.Some examples of the types of classified information agencies generate and manage include:

- Military activities
- The identities of terrorists and suspected terrorists
- Identities of intelligence agents
- Other critical issues pertaining to foreign policy and national security

Additionally, states generally maintain databases containing critical personal data from their citizenry. Individuals must supply this information when regularly interacting with agencies. All this stored information has tremendous value for potential cybercriminals. Nation-states may covet this data for intelligence purposes. Political parties or activists could benefit from breaches that damage them

opponents or further their aims. Meanwhile, others cybercriminals might seek agency data for financial gain in the form of ransom payments.

When this information is compromised, stolen, or unlawfully disclosed, the consequences can be widespread and significant across multiple sectors. That is true, not least of all due to that state agencies hold for their respective populations. Whenever there is a cybersecurity incident at the government level, it can shake citizens' confidence in their collective safety and the relative strength of their nation-state on the world stage.The fear or uncertainty inspired by one of these attacks can itself be a goal or a benefit to the attacker. Foreign powers, activists, or terrorist groups could each have reasons to undermine a populace's faith in state agencies.

They Have an Extensive Attack Surface

States almost universally have a massive attack surfacemeaning there are myriad points of vulnerability and potential exploitation throughout the sector. These points include the hundreds of thousands to millions of people, emails, devices, cloud applications, servers, and credentials that constitute state technological systems and infrastructure.Bad actors need only to find and exploit a single weakness (such as a stolen or guessed username and password) to infiltrate a network. Once a piece of a system's security is compromised, the bad actors can rapidly take advantage of further vulnerabilities and magnify the scale of their attack.The fact that many agencies still rely on legacy systems exacerbates this problem. Some agencies still run Windows 7 or an earlier version and have similarly aged client applications. Plus, it is not just a governmental department's own infrastructure that puts them at risk; it is also that of third parties. Trusted partners and contractors might suffer from many of the same deficiencies. Thus, they can extend the attack surface for governments even further.The presence of legacy systems combined with insufficient funding and a short supply of security professionals adds up to a state of low cybersecurity readiness for many institutions. Chronic failure to invest in modernizing critical cyber structures means that many of these issues have become systemic.

They Operate Critical Infrastructure

Another reason cybercriminals target state institutions are because some of them operate Critical Infrastructure Regional and local agencies, in particular, are frequently responsible for municipal facilities, transportation, communications, power supplies, and other essential services. Disruption of these vital functions due to ransomware attacks can have significant effects on individual constituents and local economies.

7. RECOVERY TIMELINE

A ransomware attack can be a harrowing experience, leaving you scrambling to regain access to your data. While prevention is paramount, knowing the potential recovery timeline can help you navigate this stressful situation. Here's a breakdown of what to expect:The initial hours are critical. Detection and Containment is the first step. Identify the affected systems, isolate them immediately to prevent the ransomware from spreading further, and assess the damage. This initial phase can take anywhere from a few hours to a day depending on the size of your network and the extent of the infection.Next comes the agonizing decision – Pay or Recover? Paying the ransom is a gamble. There's no guarantee you'll regain access to your data, and it fuels the criminal enterprise. Recovering without paying requires a solid backup strategy in place. If backups are readily available and uninfected, restoring your data can be achieved within a day or two, minimizing downtime and disruption.

Incident Response and Investigation kicks in. Security professionals will analyse the attack, identify the ransomware strain, and explore decryption tools. This process, including negotiations with potential data recovery firms, can take days or even weeks depending on the complexity of the attack.If decryption proves impossible, the recovery process shifts to data reconstruction. This involves leveraging forensic tools to analyse remnants of data on infected systems and potentially extract fragments of salvageable files. It's a painstaking effort that can take weeks or even months depending on the severity of the attack and the amount of data lost.Throughout this ordeal, Communication and Documentation are paramount. Keep stakeholders informed of the situation, document every step taken, and collaborate with law enforcement if necessary. The final stage is Post-Incident Review and Remediation.This involves patching vulnerabilities exploited by the attackers, hardening your security posture, and revisiting your backup strategy. It's crucial to learn from the experience and implement stronger defences to prevent future attacks. This phase can take weeks or even months as you rebuild your systems and implement new security measures.Remember, the timeline is highly variable. Factors like the size of your organization, the sophistication of the attack, and your preparedness all play a role. While the recovery process can be arduous, a well-defined plan and a proactive approach can significantly shorten the time it takes to regain control and minimize the impact of a ransomware attack.

8. CONCLUSION

Ransomware remains a significant cyber threat, capable of crippling businesses and causing personal devastation. However, it's not an insurmountable foe. By prioritizing robust data backups, staying vigilant with software updates and email security, and employing strong security software, you can significantly reduce your risk of infection.Furthermore, a layered approach that includes network segmentation, limited user privileges, and security awareness training bolsters your defences. Regular security testing acts as a proactive measure to identify and address weaknesses before attackers exploit them.

The key takeaway is this: prevention is far preferable to the potentially lengthy and arduous recovery process. A ransomware attack can take days to months to resolve, depending on the availability of backups, the complexity of the attack, and the chosen recovery path. The financial costs, operational disruptions, and reputational damage can be severe. By taking control of your digital security and implementing these preventative measures, you can build a formidable fortress against ransomware. Remember, your data is valuable – make it a fortress too well-guarded to be breached. In the unfortunate event of an attack, a well-defined recovery plan and a proactive approach can minimize the damage and expedite your journey back to normalcy.Through the analysis of network traffic, it is possible to identify anomalous patterns and behaviours

REFERENCES

1. FathmahAldauiji., et al. "Utilizing Cyber Threat Hunting Techniques to Find Ransomware attacks: A survey of the state of the art"(2022) : 3181278
2. Aldln Vehabovlc., et al. "Ransomware detection and classification Strategies"(2022) : 9858296
3. A.K . Maurya., et al. "Ransomware Evolution, Target and SafteyMeasures"(2017) : 10.26438
4. Felipe almeida., et al.Ransomware attack as Hardware Trojan:A fesibility and demonstration study"(2022) : 316899
5. Mansur Aliyu., et al. "Assessing The level of Cyber Security Awareness among tertiary institutions in Northern Nigeria"(2017) : 19308.